

# EXHIBIT A

NOTICE: All slip opinions and orders are subject to formal revision and are superseded by the advance sheets and bound volumes of the Official Reports. If you find a typographical error or other formal error, please notify the Reporter of Decisions, Supreme Judicial Court, John Adams Courthouse, 1 Pemberton Square, Suite 2500, Boston, MA, 02108-1750; (617) 557-1030; SJCRreporter@sjc.state.ma.us

SJC-12946

ATTORNEY GENERAL vs. FACEBOOK, INC.

Suffolk. December 4, 2020. - March 24, 2021.

Present: Budd, C.J., Gaziano, Lowy, Cypher, & Kafker, JJ.

Attorney at Law, Attorney-client relationship, Work product.  
Attorney General. Consumer Protection Act, Investigative demand. Privileged Communication.

Petition filed in the Superior Court Department on August 15, 2019.

The case was heard by Brian A. Davis, J.

The Supreme Judicial Court granted an application for direct appellate review.

Felicia H. Ellsworth for the respondent.  
Sara E. Cable, Assistant Attorney General, for the petitioner.

The following submitted briefs for amici curiae:  
Thomas O. Bean & Anuj Khetarpal for Association of Corporate Counsel.

Ariel Fox Johnson, of the District of Columbia, & Joseph Jerome for Common Sense Media.

Steven P. Lehotsky, Kevin P. Martin, William E. Evans, Ben Robbins, & Martin J. Newhouse for Chamber of Commerce of the United States of America & another.

David A. Vicinanzo, of New Hampshire, Mark Tyler Knights, Hannah R. Bornstein, & Marissa Elkins for National Association of Criminal Defense Lawyers.

Alan Butler & Megan Iorio, of the District of Columbia, & Caitriona Fitzgerald for Electronic Privacy Information Center. James M. Campbell for Lawyers for Civil Justice.

KAFKER, J. In this case we address the applicability of the attorney-client privilege and the work product doctrine to an internal investigation conducted by the respondent, Facebook, Inc. (Facebook). After public reporting revealed potential widespread misuse of Facebook user data by third-party applications (apps), Facebook hired a law firm, Gibson, Dunn & Crutcher LLP (Gibson Dunn), to conduct a far-reaching investigation to identify the extent to which apps had misused user data and advise Facebook on potential resulting legal liabilities. This investigation is known as the app developer investigation (ADI). Around the same time, the Attorney General opened an investigation into Facebook under G. L. c. 93A, focusing on whether Facebook misrepresented the extent to which it protected or misused user data.

As part of that investigation, the Attorney General served Facebook with several civil investigative demands (demands). At issue are six requests contained within these demands that sought the identities of the apps and developers that Facebook reviewed at various stages of the ADI, other information associated with the review of the identified apps, and internal

communications about those apps. Facebook asserted that both the attorney-client privilege and the work product doctrine protected this information. The Attorney General filed a petition in the Superior Court seeking an order compelling Facebook to comply with the disputed requests. A judge concluded that most of the information is neither privileged nor work product, as it was not prepared in anticipation of litigation, and that even if it was prepared in anticipation of litigation, it is all factual information.

We conclude that the Attorney General's targeted requests allow Facebook to tailor its responses to the first five of the six requests to avoid disclosure of communications protected by the attorney-client privilege. We also conclude, however, that the documents sought by the first five requests were prepared in anticipation of litigation and therefore are covered by the work product doctrine. We further conclude that a remand is required to separate "opinion" work product from "fact" work product for at least some of these documents. To the extent the work product is fact work product, we conclude that the Attorney General has satisfied the heavy burden of demonstrating a substantial need for the information. Finally, as for the sixth request, seeking internal communications about the apps, we have determined that this request encompasses both privileged and nonprivileged communications, and therefore requires preparation

of a privilege log and further review as determined by the judge.<sup>1</sup>

1. Background. a. Facebook Platform. Facebook provides social networking services through its website and mobile app. It has over 1 billion daily users and over 2 billion active accounts. Users generate a variety of data through their use of Facebook. In 2007, Facebook launched the first version of the Facebook Platform. The Platform connects Facebook users with third-party app developers and enables users to share Facebook data with the apps and developers. The Platform allows these third parties to integrate their apps with the data generated by users and collected by Facebook. For our purposes, the practical effect of the Platform is that third-party developers are given access to Facebook user data. The Attorney General alleges that over 9 million apps and websites had integrated with the Platform as of March 31, 2012.

Use of the Platform by apps and developers is governed by various policies, including Facebook's Platform policy, terms of service, and data use policy. As relevant here, these policies prohibited third-party developers from selling or licensing the

---

<sup>1</sup> We acknowledge the amicus briefs submitted by the Association of Corporate Counsel, Common Sense Media, the Chamber of Commerce of the United States and the New England Legal Foundation, the National Association of Criminal Defense Lawyers, the Electronic Privacy Information Center, and Lawyers for Civil Justice.

data they obtained from Facebook users. The policies also prohibited developers from sharing user data with "any ad network, data broker or other advertising or monetization-related service." A developer had to register to use the Platform and affirmatively agree to comply with the various policies governing use of the Platform; however, as of late 2013, apps generally could be launched on the Platform without any review or approval by Facebook.

Facebook has an internal enforcement program that monitors and responds to developer misuse of the Platform. This is known as its developer operations team.<sup>2</sup> This enforcement team monitors daily app and developer behavior with the goal of "identifying abnormalities that might signal potential policy violations." The activities of this enforcement program generally are not led by attorneys, however. In addition to monitoring compliance, this team enforces Facebook's policies according to its own rubrics and protocols. By way of illustration, Facebook estimates that it took enforcement action against about 370,000 apps in 2017 as a result of these routine enforcement efforts.

---

<sup>2</sup> Among the impounded materials in this case are detailed descriptions of the developer operations team provided to the Attorney General by Facebook.

In April 2014, Facebook revised its Platform and the accompanying policies to improve protections for user data.<sup>3</sup> These changes "enhance[d] users' ability to control app developers' access to their information." Specifically, they restricted the categories of information apps could access and gave users more tools to limit the type of information apps could access. Facebook also added a screening mechanism that required apps and developers to obtain Facebook's approval before getting access to many advanced categories of user data. After this screening mechanism was put in place, Facebook rejected the requests of roughly fifty percent of apps that sought access to the additional user data.

b. Cambridge Analytica incident. In March 2018, several news outlets reported on an incident involving Facebook, an individual named Aleksandr Kogan, and a company named Cambridge Analytica. Briefly, Kogan used an app on the prior version of the Platform to access and collect the data of as many as 87 million Facebook users worldwide, roughly 70 million of whom were located in the United States. Kogan sold this data to Cambridge Analytica, a political data analytics and advertising firm, and other related entities. Cambridge Analytica used this

---

<sup>3</sup> Facebook formally refers to the version of the Platform that was in effect before these changes as "Graph API v. 1.0." We refer to it as the "prior version" of the Platform.

data to create "psychographic profiles" on the Facebook users. Cambridge Analytica then used these profiles to target Facebook users with political advertising. According to Facebook, this conduct violated the Platform policies described above in multiple ways.<sup>4</sup>

The 2018 reporting of this incident sparked a wave of litigation against and investigations into Facebook. By the end of 2018, Facebook faced at least five securities class actions, eight derivative actions, three books and records actions, and thirty-nine consumer-based suits, most of which also were class actions.<sup>5</sup> This number swelled to at least sixty-five litigations before the end of 2019. Facebook is also being investigated by a number of State, Federal, and foreign regulators.

---

<sup>4</sup> Facebook first learned that Kogan and Cambridge Analytica had accessed the data in December 2015, again from public reporting. At that point, Facebook suspended Kogan's app from the Platform. It did not ban Cambridge Analytica from the Platform at that time. Facebook also did not disclose the violations to the users whose information was implicated at the time. Instead, Facebook only pursued enforcement action against Kogan and obtained assurances that Kogan and Cambridge Analytica had deleted all of the improperly collected data. The subsequent reporting in 2018 revealed that, contrary to those representations, Cambridge Analytica had not deleted the Facebook user data.

<sup>5</sup> All but one of these consumer lawsuits have been consolidated in a multidistrict litigation in the United States District Court for the Northern District of California. See *In re: Facebook, Inc., Consumer Privacy User Profile Litigation*, U.S. Dist. Ct., No. 18-md-02843-VC, MDL No. 2843 (N.D. Cal.).



c. ADI.<sup>6</sup> Facebook launched the ADI investigation soon after the reporting on Cambridge Analytica in March 2018. According to Facebook, the purpose of the ADI is to "gather the facts necessary for providing legal advice to Facebook about litigation, compliance, regulatory inquiries, and other legal risks facing the company resulting from potential data misuse and activities by third-party app developers operating on the prior version of the Platform." The goal of the ADI, therefore, is to identify any other apps that misused user data on the prior version of the Platform and assess Facebook's potential legal liability as a result of any uncovered misuse. Facebook states that the ADI has been "designed, managed, and overseen" by Gibson Dunn and Facebook's in-house counsel, and these attorneys "devised and tailored the ADI's methods, protocols, and strategies to address the specific risks posed by these legal challenges." Gibson Dunn recruited and retained the outside technical experts and investigators involved in the ADI.

Counsel also developed the framework for the ADI. In broad terms, the ADI consists of three separate phases. The first phase focuses on detection and identification. The goal of this phase is either to elevate an app or developer for closer investigation or to exclude apps that pose less risk. Using

---

<sup>6</sup> Some details regarding the ADI are impounded. Therefore, our discussion of the ADI here does not include certain details.

four different methods, Facebook has reviewed millions of apps and determined which ones should be investigated further.<sup>7</sup> If an app is identified by one of the methods used during the first phase, then the app warrants further review by the ADI team. The second phase focuses on enhanced examination. This phase involves "background" or "technical" investigations of the apps escalated in the first phase. The third phase involves engagement with, and potentially enforcement against, apps or developers that violated Facebook's policies.

The ADI involves various types of personnel. Facebook's in-house legal team and Gibson Dunn hired multiple forensic consulting firms to assist with the investigation. At times, the ADI has included as many as 300 internal and external experts. Despite the number of people involved in the investigation, Facebook represents that it has taken various steps to ensure that the ADI remains confidential. This includes limiting communications about the investigation and restricting access to documents.

---

<sup>7</sup> The four methods are (1) the user-impact method, in which apps with a large number of installing users are prioritized for review; (2) the categorical method, in which the ADI investigative team, relying on past investigative experience, groups apps and developers into categories and prioritizes them for review; (3) the escalations method, in which apps are prioritized based on information from other sources, both internally and externally; and (4) the low impact method, in which apps that do not pose as much legal risk as others are deprioritized for review.

d. Attorney General's investigation. Shortly after the media coverage of the Cambridge Analytica incident in March 2018, the Attorney General began investigating Facebook under G. L. c. 93A, § 6. The purpose of the investigation is to identify any other apps that misused user data and assess whether Facebook followed its policies and commitments to its users regarding user data. Over the course of the investigation, the Attorney General has issued three demands. The first demand was issued in April 2018. The second demand, issued in June 2018, sought information on the apps that Facebook had suspended and information on Facebook's internal policies and procedures surrounding apps. As part of its response, Facebook provided the Attorney General with detailed information on how it has conducted the ADI.

The third demand, issued on November 5, 2018, is the subject of this dispute. In this demand, the Attorney General sought the identities of and information regarding the apps and developers that Facebook identified and reviewed as part of the ADI. Specifically, the Attorney General took the detailed descriptions of the ADI that Facebook provided and used that language in her requests. In response, Facebook provided updated information on suspended apps but refused to comply with several of the requests.

There are six contested requests at the center of this dispute. The judge below described these requests as follows:

"1. The group of 6,000 apps with a large number of installing users<sup>[8]</sup> . . . ;

"2. The group of apps and developers that fall within certain categories that, based on Facebook's 'past investigative experience,' present an elevated risk of potential policy violations . . . ;

"3. The group of apps and developers that were reported to Facebook from outside of the ADI process, such as through the Data Abuse Bounty Program (to the extent not already produced), media reporting and inquiries, and other referrals from internal Facebook teams . . . ;<sup>[9]</sup>

"4. The group of apps and/or developers on which, to date, Facebook has conducted a 'detailed background check . . . to gauge whether the app or developer has engaged in behavior that may pose a risk to Facebook user data or raise suspicions of data misuse, to identify connections with other entities of interest, and to search for any other indications of fraudulent activity' . . . ;

"5. The group of apps on which, to date, Facebook has conducted a 'technical review' to analyze 'available technical information about the apps derived from Facebook's available internal usage records in order to gauge data collection practices -- such as the disproportionate collection of data and broad data requests -- which may suggest data misuse' . . . ; and

---

<sup>8</sup> The apps sought in the first request were not simply the apps that had the largest number of installing users; these apps were selected using a combination of factors, including the number of installing users and permissions to certain types of data.

<sup>9</sup> The data abuse bounty program provides third parties an avenue to refer apps that may have engaged in wrongful conduct to Facebook. Facebook has complied with this portion of the first contested request and identified apps and developers flagged through this program.

"6. All of Facebook's internal communications and internal correspondence concerning the apps that 'had access to large amounts of Facebook data before the 2014 changes to [Facebook's] Platform took effect,' and/or for which Facebook has conducted an 'in-depth review,' a 'Background Information Investigation' or a 'Technical Investigation.'"

The first five requests require Facebook to produce documents sufficient to identify the apps and facts concerning them (app information). Specifically, the first five requests seek the identity of all the apps described in the requests. For some of the apps, the Attorney General also seeks the following additional factual information: the app developer or publisher; whether the app was released to the public; the date the app was first released to the public; the date Facebook first reviewed the app's privacy policy; the "basis and initial source(s) of reports, allegations or concerns of data misuse of user information obtained or accessed through the app"; the categories of user information for which the app obtained permissions; the number of users who downloaded or installed the app; and the number of users who did not download or install the app but whose information was still accessed or obtained by the app.

For each of these five requests, the Attorney General provided that "[i]n lieu of documents in response to this Request, the Commonwealth will accept information in a spreadsheet format." Facebook therefore is not required to

produce any existing documents sent to or created by the ADI team in regard to the first five requests; rather, it simply is required to assemble a list of apps that is responsive to each request and provide the additional requested information concerning those apps. The sixth request is different, however; it seeks internal communications about many of those apps.

e. Prior productions. Throughout the investigation, Facebook has engaged extensively with the Attorney General. Facebook has provided the Attorney General with the name of every app and developer that it has suspended from the Platform.<sup>10</sup> Similarly, Facebook provided the Attorney General with the identities of any developers that it sought to interview or audit or from which it requested information. Facebook has also provided the Attorney General with numerous narrative responses at various stages of the investigation. As part of these narratives, Facebook has provided the Attorney General with a detailed overview of the ADI and a general summary of the criteria used in each phase. Throughout its engagement with the Attorney General, Facebook emphasized that

---

<sup>10</sup> Only one app -- Kogan's app -- has been suspended for actual misuse of user data. When it provided the identities of other suspended apps, Facebook did not explain why it suspended each app. Instead, it provided general explanations for why groups of apps were suspended, which was often because of their affiliation with a particular developer.

it was not waiving any applicable privilege over the investigation.

Facebook also has produced at least 15,000 documents across seven productions in response to the third demand. This includes communications with developers and requests for information. Similarly, Facebook has met with the members of the Attorney General's investigative team on numerous occasions.

f. Public statements about ADI. Facebook has made several public statements about the ADI since its inception. Facebook publicly announced its investigation into the Kogan incident on March 21, 2018. In this statement, Facebook said, "We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity. If we find developers that misused personally identifiable information, we will ban them from our platform." It also said that it would "tell people affected by apps that have misused their data" and expand its program for rewarding people who report data misuse by app developers.

In the months that followed, Facebook made other public statements about the ADI. On April 11, 2018, Mark Zuckerberg, the chief executive officer of Facebook, testified before Congress, stating,

"We're in the process of investigating every app that had access to a large amount of information before we locked down our platform in 2014. If we detect suspicious activity, we'll do a full forensic audit. And if we find that someone is improperly using data, we'll ban them and tell everyone affected."

He also told Congress that, at that time, "around 200 apps . . . from a handful of developers" had been suspended pending investigation into whether they misused data.

Facebook provided a more detailed public update on the ADI in a press release in May 2018:

"The investigation process is in full swing, and it has two phases. First, a comprehensive review to identify every app that had access to this amount of Facebook data. And second, where we have concerns, we will conduct interviews, make requests for information (RFI) -- which ask a series of detailed questions about the app and the data it has access to -- and perform audits that may include on-site inspections.

"We have large teams of internal and external experts working hard to investigate these apps as quickly as possible. To date thousands of apps have been investigated and around 200 have been suspended -- pending a thorough investigation into whether they did in fact misuse any data. Where we find evidence that these or other apps did misuse data, we will ban them and notify people via this website. It will show people if they or their friends installed an app that misused data before 2015 -- just as we did for Cambridge Analytica."

Facebook provided another public update in August 2018. It stated that it had suspended an app "for failing to agree to our request to audit and because it's clear that [the app] shared information with researchers as well as companies with only limited protections in place." Facebook also informed the



public, "Since launching our investigation in March, we have investigated thousands of apps. And we have suspended more than 400 due to concerns around the developers who built them or how the information people chose to share with the app may have been used -- which we are now investigating in much greater depth."

Finally, in September 2019, Facebook announced:

"We wanted to provide an update on our ongoing [ADI], which we began in March of 2018 as part of our response to the episode involving Cambridge Analytica.

". . .

"We initially identified apps for investigation based on how many users they had and how much data they could access. Now, we also identify apps based on signals associated with an app's potential to abuse our policies. Where we have concerns, we conduct a more intensive examination. This includes a background investigation of the developer and a technical analysis of the app's activity on the platform. Depending on the results, a range of actions could be taken from requiring developers to submit to in-depth questioning, to conducting inspections or banning an app from the platform. . . .

"To date, this investigation has addressed millions of apps. Of those, tens of thousands have been suspended for a variety of reasons while we continue to investigate.

"It is important to understand that the apps that have been suspended are associated with about 400 developers. This is not necessarily an indication that these apps were posing a threat to people. Many were not live but were still in their testing phase when we suspended them. It is not unusual for developers to have multiple test apps that never get rolled out. And in many cases, the developers did not respond to our request for information so we suspended them, honoring our commitment to take action.

"In a few cases, we have banned apps completely. That can happen for any number of reasons including inappropriately sharing data obtained from us, making data publicly

available without protecting people's identity or something else that was in clear violation of our policies. We have not confirmed other instances of misuse to date other than those we have already notified the public about, but our investigation is not yet complete. We have been in touch with regulators and policymakers on these issues. We'll continue working with them as our investigation continues."

g. Procedural history. In August 2019, the Attorney General filed a petition to compel compliance with the third demand in the Superior Court. Facebook opposed the petition, arguing that the requests sought information protected by the attorney-client privilege and work product doctrine. A hearing was held on the petition on November 7, 2019.

In January 2020, a Superior Court judge largely granted the Attorney General's petition. He first concluded that the work product doctrine did not apply because the ADI was a continuation of Facebook's ongoing app enforcement program, rather than done in anticipation of litigation. He also concluded that even if the app information was work product, it nonetheless was discoverable because it constituted fact work product and the Attorney General had demonstrated a substantial need for the information. The judge then concluded that the attorney-client privilege did not apply to most of the information sought because the app information was factual in nature and because Facebook had "touted" the ADI in public and therefore could not claim a privilege over the investigation. The judge further concluded that the wording of the sixth

request was broad enough that it likely sought some privileged communications that included "requests for legal advice and/or legal advice on the part of Facebook and its attorneys . . . ." He emphasized that he was not compelling the production of such communications and ordered Facebook to prepare a detailed privilege log so that the Attorney General could challenge any assertions of privilege. Facebook appealed, and we granted its application for direct appellate review.<sup>11</sup>

2. Discussion. a. Waiver of objections to demand.

Before reaching the merits, we first address the Attorney General's argument that Facebook has waived its objections to the third demand by failing to move to modify or set it aside under G. L. c. 93, § 6 (7). The Attorney General argues that § 6 (7), as well as our decision in Attorney Gen. v. Bodimetric Profiles, 404 Mass. 152 (1989) (Bodimetric), require recipients of demands to file such a motion to preserve any objections to a demand, something that Facebook did not do here.

In Bodimetric, we held that "failure to bring such a motion pursuant to [§ 6 (7)] constitutes a waiver by the person to whom the [demand] is served." Bodimetric, supra at 154. The recipient of the demand in that case refused to comply with it

---

<sup>11</sup> Facebook's attempts to stay the judge's order pending appeal were unsuccessful. Facebook has been producing the app information and communications to the Attorney General subject to a protective order during the pendency of this appeal.

and merely sent a letter stating its objections to the Attorney General. Id. at 155. We further explained that "[t]he recipient [of a demand] may not remain passive . . . raising legal arguments only after the Attorney General brings a motion to compel." Id. Despite the fact that the recipient had "[sent] a letter to the Attorney General stating its objections to the [demand,] . . . [m]erely informing the Attorney General of its refusal to comply [did] not suffice to shift the burden to the Attorney General to take the next legal step." Id. The judge below rejected this argument, concluding that, under Bodimetric, a judge has the discretion to deem a failure to file a timely motion for relief as a waiver of the right to object to the demand but is not obligated to do so. The judge then determined that Facebook had not waived its right to object to the demand.

We agree that Facebook has not waived its objections to the demand. Whereas the recipient of the demand in Bodimetric refused to comply altogether, Facebook's engagement with the Attorney General has been far from passive. Instead, Facebook has worked with the Attorney General and communicated its objections to the third demand, including its assertions of privilege. Facebook has also complied with the requests in the demand that Facebook believes call for nonprivileged information. Moreover, finding waiver here could discourage

cooperation with the Attorney General and result in increased litigation whenever the Attorney General serves a demand. We therefore conclude that Facebook has not waived its objections to the demand.

b. Legal standards. This case implicates both the attorney-client privilege and the work product doctrine. We review the applicability of both de novo. Commissioner of Revenue v. Comcast Corp., 453 Mass. 293, 302 (2009) (Comcast). Facebook, as the party asserting the protections, bears the burden of proving that both the privilege and the work product doctrine apply. Id. at 304. See Clair v. Clair, 464 Mass. 205, 215 (2013) ("The party asserting attorney-client privilege has the burden of establishing that the privilege applies to the communications at issue").

c. Attorney-client privilege. We begin with the attorney-client privilege. The attorney-client privilege protects "all confidential communications between a client and its attorney undertaken for the purpose of obtaining legal advice." Suffolk Constr. Co. v. Division of Capital Asset Mgt., 449 Mass. 444, 448 (2007). See Comcast, 453 Mass. at 303 (elements of privilege). See also Mass. G. Evid. § 502(b) (2021).<sup>12</sup> The

---

<sup>12</sup> The attorney-client privilege applies to corporations. See Upjohn Co. v. United States, 449 U.S. 383, 389-390 (1981). Indeed, "the attorney-client privilege for business organizations [is] essential in light of 'the vast and

privilege covers the flow of confidential communications in both directions -- from the attorney to the client and from the client to the attorney -- as the "purpose of the privilege 'is to enable clients to make full disclosure to legal counsel of all relevant facts . . . so that counsel may render fully informed legal advice,' with the goal of 'promot[ing] broader public interests in the observance of law and administration of justice.'" Comcast, supra, quoting Suffolk Constr. Co., supra at 449. We have emphasized the value of protecting confidential attorney-client communications, as the "social good derived from the proper performance of the functions of lawyers acting for their clients . . . outweigh[s] the harm that may come from the suppression of the evidence." Hanover Ins. Co. v. Rapo & Jepsen Ins. Servs., Inc., 449 Mass. 609, 615-616 (2007), quoting Commonwealth v. Goldman, 395 Mass. 495, 502, cert. denied, 474 U.S. 906 (1985). See Matter of a Grand Jury Investigation, 437 Mass. 340, 351 (2002) (Grand Jury Investigation) ("Considerable public benefit inures when an institution voluntarily scrutinizes its own operations for the purpose of seeking advice from counsel on how to comply with the law, particularly where today's increasingly dense regulatory terrain makes such

---

complicated array of regulatory legislation confronting the modern corporation.'" In re Kellogg Brown & Root, Inc., 756 F.3d 754, 757 (D.C. Cir. 2014), cert. denied, 574 U.S. 1122 (2015), quoting Upjohn Co., supra at 392.

compliance 'hardly an instinctive matter'). "A construction of the attorney-client privilege that would leave internal investigations wide open to third-party invasion would effectively penalize an institution for attempting to conform its operations to legal requirements by seeking the advice of knowledgeable and informed counsel." Grand Jury Investigation, supra.

Despite the strong protections given to material subject to the attorney-client privilege, "[w]e consistently have held that the privilege is to be construed narrowly." Clair, 464 Mass. at 215, citing Comcast, 453 Mass. at 304. We do so because the privilege "frustrate[s] the investigative or fact-finding process . . . [and] create[s] an inherent tension with society's need for full and complete disclosure of all relevant evidence during implementation of the judicial process'" (citation omitted). Comcast, supra. See Hanover Ins. Co., 449 Mass. at 615, quoting In re Grand Jury Investigation No. 83-2-35, 723 F.2d 447, 451 (6th Cir. 1983), cert. denied, 467 U.S. 1246 (1984). See also Lluberes v. Uncommon Prods., LLC, 663 F.3d 6, 24 (1st Cir. 2011) ("attorney-client privilege must be narrowly construed because it comes with substantial costs and stands as an obstacle of sorts to the search for truth" [citation omitted]). We also have recognized that the privilege can be waived. Comcast, supra at 303.

In balancing these competing concerns and determining whether the privilege applies, we focus on the distinctions between attorney-client communications and underlying facts. As we explained in Chambers v. Gold Medal Bakery, Inc., 464 Mass. 383, 392 (2013):

"[The distinction between communications and underlying facts] is crucial because attorney-client privilege only protects against disclosure of confidential communications made to render legal services. [Comcast, 453 Mass. at 305]. It does not immunize underlying facts available from another source from discovery just because a client disclosed the facts to an attorney. See M.S. Brodin & M. Avery, Massachusetts Evidence § 5.4.4 (8th ed. 2007 & Supp. 2013), quoting Upjohn Co. v. United States, 449 U.S. 383, 395-396 (1981) [Upjohn] ('A fact is one thing and a communication concerning that fact is an entirely different thing')."

In Upjohn, supra, the United States Supreme Court explained this distinction:

"The privilege only protects disclosure of communications; it does not protect disclosure of the underlying facts by those who communicated with the attorney: '[T]he protection of the privilege extends only to communications and not to facts. . . . The client cannot be compelled to answer the question, "What did you say or write to the attorney?" but may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of such fact into his communication to his attorney.' . . . Here, the Government was free to question the employees who communicated with [the company's lawyer] and outside counsel." (Emphasis in original; citation omitted.)

This distinction is important and somewhat collapsed by the advocacy in the instant case. Facebook interprets the requests as seeking confidential communications between Facebook and its



outside counsel or information that does not exist independently of such communications. This fails to take into account the fact that the underlying data about apps' breaches of privacy policies is all independently discoverable and cannot be protected by Facebook's initiation of its own factual investigation. The attorney-client privilege only protects communications between the attorney and the client about such factual information, not the facts themselves.

i. First five requests. The first five requests do not require the production of any communications between Facebook and counsel during the ADI process.<sup>13</sup> Rather, these requests only seek documents "sufficient to identify" the apps that fall within the five categories of requested documents identified supra or lists of the apps themselves, and other information associated with those apps. While this certainly requires the production of factual information relevant to the Attorney General's investigation, and such factual information has almost certainly been contained in attorney-client communications, it does not require the production of the attorney-client communications themselves. This is a crucial distinction; as the Supreme Court explained in Upjohn, 449 U.S. at 396, a client "may not refuse to disclose any relevant fact within his

---

<sup>13</sup> On the other hand, the sixth contested request, which we address infra, explicitly seeks communications.

knowledge merely because he incorporated a statement of such fact into his communication to his attorney" (citation omitted).

The app information sought by the Attorney General in the first five requests differs from the type of information that has been deemed covered by the attorney-client privilege. For example, Upjohn involved responses to questionnaires and interview notes that included responses to questions. See Upjohn, 449 U.S. at 397. Corporate employees communicated factual information to the corporation's attorneys in response to requests from the attorneys for information. The Court held that such communications of factual information were covered by the privilege. Id. at 395. Similarly, in Federal Trade Comm'n v. Boehringer Ingelheim Pharms., Inc., 180 F. Supp. 3d 1, 30-32 (D.D.C. 2016) (Boehringer III), aff'd, 892 F.3d 1264, 1266 (D.C. Cir. 2018) (Boehringer IV), the court held that the privilege shielded, among other things, PowerPoint presentations and spreadsheets that summarized facts and analyzed how various litigation and settlement outcomes would have an impact on the company financially. Company employees prepared the documents and sent them to the company's general counsel at her request to assist her with settlement negotiations. Boehringer III, supra at 32. In affirming the conclusion that the documents were privileged, the United States Court of Appeals for the District of Columbia Circuit emphasized:

"[T]he attorney-client privilege 'only protects disclosure of communications' . . . . [It] does not prevent the [Federal Trade Commission's] discovery of the underlying facts and data possessed by [the company] and its employees. . . . But [it] does protect the communication of facts by corporate employees to the general counsel when . . . the communications were for the purpose of obtaining or providing legal advice" (emphasis in original).

Boehringer IV, supra at 1268.

In the first five requests, the Attorney General is not requiring the production of documents or communications that were exchanged between Facebook (including its employees) and its attorneys, and the requests permit Facebook to comply without disclosing any such communications. Therefore, Facebook cannot rely on the attorney-client privilege as a basis for refusing to comply with these requests. We reiterate that "[t]he client cannot be compelled to answer the question, 'What did you say or write to the attorney,'" particularly where those communications occur during an internal investigation (citation omitted). See Upjohn, 449 U.S. at 396. Facebook is not being compelled to answer those questions, however, and it does not have to produce any communications with its attorneys. Given the flexibility provided to Facebook in its response, the factual information it is required to produce in response to the first five requests is thus not covered by the attorney-client privilege. As will be explained infra, however, as framed, the requests do implicate the work product doctrine.

ii. Sixth request. The sixth request broadly seeks "[a]ll of Facebook's internal communications and internal correspondence concerning" several categories of apps sought in the other requests. Facebook refused to comply with this request and asserted that it called for the production of privileged communications. The judge below ordered Facebook to produce a detailed privilege log identifying any documents it was withholding on the basis of the privilege. While this case proceeded on appeal, Facebook provided the Attorney General with at least two privilege logs responsive to this request.<sup>14</sup>

As explained above, the attorney-client privilege certainly applies to communications between counsel and client made as part of an internal investigation that is undertaken to gather facts for the purposes of providing legal advice. See, e.g., Grand Jury Investigation, 437 Mass. at 351. See also Upjohn, 449 U.S. at 390. The ADI is such an investigation, as it was initiated in part to gather the facts needed to advise Facebook on various legal risks facing the company. See Comcast, 453 Mass. at 303 (elements of privilege). As such, any confidential communications relating to the ADI among Facebook, Gibson Dunn, and other members of the ADI team would almost certainly be

---

<sup>14</sup> In one log, Facebook identified seven categories for which it is withholding documents on a categorical basis. This includes 40,108 documents. The other log contained 947 entries over which Facebook is asserting the privilege.

privileged. There may also be other responsive communications between counsel and client outside the ADI that are privileged. At the same time, the breadth of the request includes communications outside the ADI that may not otherwise involve attorney-client communications. The Attorney General is seeking communications dating back to April 30, 2014, which is years before the ADI began in the spring of 2018.<sup>15</sup> The request, on its face, also applies to communications between Facebook employees who are not lawyers and are not acting at the direction of lawyers. Further sorting out of this request is required.

We therefore agree with the judge below that the appropriate course of action is for Facebook to prepare a detailed privilege log so that the Attorney General can challenge any assertions of privilege.

d. Work product doctrine. Facebook also argues that the app information requested is protected by the work product doctrine. The work product doctrine "protects (1) 'documents and tangible things,' [prepared] (2) 'by or for another party or by or for that other party's representative (including his

---

<sup>15</sup> Facebook represents that it "has never claimed that the privilege derived from the [ADI] attaches to pre-[ADI] communications." Rather, "it has only withheld pre-[ADI] communications to the extent they are privileged on other grounds."

attorney, consultant, surety, indemnitor, insurer, or agent), ' and (3) 'in anticipation of litigation or for trial.'" McCarthy v. Slade Assocs., Inc., 463 Mass. 181, 194 (2012), quoting P.M. Lauriat, S.E. McChesney, W.H. Gordon, & A.A. Rainer, *Discovery* § 4:5 (2d ed. 2008 & Supp. 2011).<sup>16</sup> Importantly, "[t]he work product protection is broader than the attorney-client privilege in that it is not restricted solely to confidential communications between an attorney and client." Federal Trade Comm'n v. Boehringer Ingelheim Pharms., Inc., 778 F.3d 142, 149 (D.C. Cir. 2015) (Boehringer II), cert. denied, 577 U.S. 1102 (2016).<sup>17</sup> "The purpose of the doctrine is to establish a 'zone

---

<sup>16</sup> Rule 26 (b) (3) of the Massachusetts Rules of Civil Procedure, 365 Mass. 772 (1974), states:

"Subject to the provisions of subdivision (b) (4) of this rule, a party may obtain discovery of documents and tangible things otherwise discoverable under subdivision (b) (1) of this rule and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including his attorney, consultant, surety, indemnitor, insurer, or agent) only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of his case and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation."

<sup>17</sup> At the same time, it is also narrower than the attorney-client privilege, as it only protects documents prepared in anticipation of litigation. Boehringer II, 778 F.3d at 149.

of privacy for strategic litigation planning . . . to prevent one party from piggybacking on the adversary's preparation.'" Comcast, 453 Mass. at 311-312, quoting United States v. Adlman, 68 F.3d 1495, 1501 (2d Cir. 1995).

A document is prepared in anticipation of litigation if, "in light of the nature of the document and the factual situation in the particular case, the document can be fairly said to have been prepared because of the prospect of litigation" (emphasis added). Comcast, 453 Mass. at 317, quoting United States v. Adlman, 134 F.3d 1194, 1202 (2d Cir. 1998) (Adlman II). Anticipation of litigation does not have to be the primary purpose or motivation. Comcast, supra at 317 n.28. But a document that would have been prepared "irrespective of the prospect of litigation" is not covered by the work product doctrine (citation omitted). Id. at 318-319. See Adlman II, supra at 1202 ("documents that are prepared in the ordinary course of business or that would have been created in essentially similar form irrespective of the litigation" not covered).

If the work product doctrine applies, the court must determine what type of work product is at issue. Rule 26 (b) (3) differentiates between two types of work product. The greatest protection is provided to opinion work product, or work product that conveys the "mental impressions, conclusions,

opinions, or legal theories of an attorney or other representative of a party concerning the litigation." See Mass. R. Civ. P. 26 (b) (3), 365 Mass. 772 (1974). Opinion work product "may be reflected in interviews, statements, memoranda, correspondence and in countless other tangible and intangible ways." Miller v. Holzmann, 238 F.R.D. 30, 32 (D.D.C. 2006). See Securities & Exch. Comm'n v. Collins & Aikman Corp., 256 F.R.D. 403, 410 (S.D.N.Y. 2009) (opinion work product "constitutes legal documents drafted by an attorney -- her mental impressions, conclusions, opinions, and legal theories"). Opinion work product is only discoverable, if at all, "in rare or 'extremely unusual' circumstances." Comcast, 453 Mass. at 315, quoting Reporters' Notes to Rule 26 (b) (3), Mass. Ann. Laws Court Rules, Rules of Civil Procedure, at 545 (LexisNexis 2008).

In contrast, all other work product is discoverable "upon a showing that the party seeking discovery has substantial need of the materials . . . and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means." Mass. R. Civ. P. 26 (b) (3). This type of work product is often referred to as fact work product. See Comcast, 453 Mass. at 314 (differences between opinion and fact work product); Cahaly v. Benistar Prop. Exch. Trust Co., 85 Mass. App. Ct. 418, 425 (2014) (same). Although it is discoverable in



some circumstances, fact work product is still protected so that "each side must undertake its own investigation of the relevant facts and not simply freeload on opposing counsel." Boehringer II, 778 F.3d at 156.

The line between fact work product and opinion work product is not always clear. Indeed, "[w]hen a factual document selected or requested by counsel exposes the attorney's thought processes and theories, it may be appropriate to treat the document as opinion work product, even though the document on its face contains only facts." Id. at 151. Yet "not every item which may reveal some inkling of a lawyer's mental impressions, conclusions, opinions, or legal theories is protected as opinion work product." In re San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d 1007, 1015 (1st Cir. 1988). The focus, selection, or arrangement of the facts must reflect the attorney's thought process in some "meaningful way." Boehringer II, supra. See Boehringer III, 180 F. Supp. 3d at 26, quoting Boehringer II, supra at 152 (fact information is not opinion work product where "[n]one of the documents reveal[s] how [the attorney] analyzed the data she requested or what data or scenarios she presented to her client. In other words, she did not 'sharply focu[s] or wee[d]' the facts contained in these documents such that revealing these facts would reveal her legal impressions of the case"). Importantly, where a document contains both fact and

opinion work product, a court may still order its production if the opinion portions can be redacted or removed. Boehringer II, supra.<sup>18</sup> Ultimately, as long as disclosing the information would not reveal an attorney's "mental impressions, conclusions, opinions, or legal theories," it is not entitled to near-absolute protection and is subject to disclosure upon a showing of substantial need and undue hardship. See Mass. R. Civ. P. 26(b) (3).

Applying these principles, we conclude that the app information required to be produced is clearly covered by the work product doctrine. We also conclude that if this app information is not opinion work product, Facebook must disclose that information, because the Attorney General has demonstrated a substantial need for the information and could not obtain it without undue hardship. The difficult issue is separating fact from opinion work product in the first five requests. We set

---

<sup>18</sup> In other words, information may appropriately be treated as fact work product if it can be produced in a format that removes any portions that contain attorney opinions, thoughts, or conclusions. See McCarthy, 463 Mass. at 197-198 & n.34. See also Washington Bancorp. v. Said, 145 F.R.D. 274, 278-279 (D.D.C. 1992) (index was discoverable fact work product even though it contained some opinion work product that could be redacted or removed prior to production).

out the mode of analysis here but remand to the judge its application to the specific requests.<sup>19</sup>

i. In anticipation of litigation. We begin with the threshold question whether the information is protected by the work product doctrine. In assessing whether the app information required to be produced is work product, the parties focus on the third element -- whether the app information was prepared "in anticipation of litigation." The judge below did as well, concluding that Facebook's existing app enforcement efforts and its public statements about the ADI demonstrate that the ADI was not done in anticipation of litigation.

We disagree with the judge on this point. We recognize that the existence of an ongoing compliance program is an important consideration when assessing whether an internal investigation was undertaken in anticipation of litigation. Indeed, simply funneling an organization's investigation through outside counsel does not bring with it the protection of the work product doctrine if the organization would have conducted these activities irrespective of anticipated litigation. See, e.g., In re Premera Blue Cross Customer Data Sec. Breach Litig.,

---

<sup>19</sup> We recognize that the Attorney General is "piggy-backing" on the extensive factual and technical investigation undertaken by Facebook rather than attempting to engage in this enormous investigation herself. While normally prohibited, rule 26 permits such piggy-backing where there is a substantial need and undue hardship.

296 F. Supp. 3d 1230, 1245-1246 (D. Or. 2017) (merely directing consultant to report to outside counsel and label communications "privileged" or "work product" insufficient to treat reports created as in anticipation of litigation).

Here, however, the ADI is meaningfully distinct from Facebook's ongoing enforcement program. It is staffed by outside counsel and outside forensic consultants, and it has its own distinct methodology. It is focused on past violations, not ongoing operations, and it serves a very different purpose: defending Facebook against the vast litigation it is facing, rather than just improving its ongoing operations. The record here does not support the contention that Facebook's compliance and enforcement team could have or would have conducted a massive investigation into potential past misconduct in the ordinary course of business.<sup>20</sup> This was not business as usual for Facebook.

The Attorney General argues that "the purpose of the ADI was to improve the Platform and remedy the loss of user trust" and not because of impending litigation. The fact that the ADI also serves business purposes does not alter the analysis. In Comcast, 453 Mass. at 317 n.28, we rejected a formulation of the

---

<sup>20</sup> Tellingly, Facebook did not initiate an investigation when it first learned of Kogan's misconduct in 2015. Instead, it waited until substantial public reporting in 2018 made litigation and regulatory investigations a near certainty.

work product doctrine that excludes documents that were primarily prepared for a business or other nonlitigation purpose. Instead, we made clear that the work product doctrine applies as long the corporation "had 'the prospect of litigation in mind.'" Id. at 318, quoting Adlman II, 134 F.3d at 1204. See Comcast, supra at 319 (documents "created 'because of' the reasonability possibility of litigation" covered by doctrine). That the ADI also serves Facebook's business purposes independent of litigation, therefore, does not mean that the work product doctrine does not apply.

The determinative question is whether Facebook compiled the app information because of the prospect of litigation or whether it would have compiled the app information regardless of the prospect of litigation. See Comcast, 453 Mass. at 318-319 (document prepared "irrespective of the prospect of litigation" is not covered by work product doctrine). Given the focus of the ADI, its structure and design, and its litigation purposes, we conclude that Facebook has established that the ADI was initiated, and the app information compiled, in anticipation of litigation. Therefore, the app information is work product.

ii. Fact or opinion work product. The next issue is whether the app information is properly considered opinion work product, which is only discoverable in extreme circumstances, or fact work product, which is discoverable if the Attorney General

demonstrates a substantial need and undue hardship. See Mass. R. Civ. P. 26 (b) (3). The judge below concluded that the app information is not opinion work product, because the requests seek "indisputably factual information" like the identity of apps or developers. Facebook counters that "but for the involvement, analysis, and advice of counsel, the [app information] the Attorney General seeks would not exist," because it is the product of "criteria designed by, and reflecting the legal judgment of, Facebook's counsel." For this reason, Facebook argues that the app information should be considered opinion work product.

In deciding whether this is opinion work product, we focus on what the specific information requested would reveal and not on the ADI as a whole. We also focus on what the requested information would divulge about the confidential as opposed to the publicly revealed aspects of the ADI process, that is, whether the documents required to be produced reveal confidential aspects of the ADI process or just those publicly announced.

We begin with the recognition that the underlying factual information about the apps, and the potential privacy violations, that the Attorney General sought was not protected by the work product doctrine. Had Facebook not informed the Attorney General how it conducted its own factual investigation,

the Attorney General would have been free to perform her own thorough investigation of all the underlying factual information to uncover data misuse by apps.

The requests, however, do seek the names of the apps, and other associated information, identified by Facebook's own investigatory process. They do so tracking Facebook's own methodology and public disclosures. This clearly asks for work product; the only question is whether it is fact or opinion work product.

In answering this question, we focus on the flexibility allowed in the response, the particular factual information requested, and the previous public disclosures. As drafted, the requests allow Facebook to tailor its response to remove any and all notes, impressions, and legal analysis except the names themselves and the specific additional factual information requested, and what those names and this additional factual information themselves reveal. See In re Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d 844, 846 (8th Cir. 1988) (tape was not opinion work product where it "d[id] not itself contain counsel's mental impressions, conclusions or legal theories"); In re San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d at 1014 (opinion work product "encompass[ed] materials that contain the mental impressions, conclusions, opinions or

legal theories of an attorney"; rest was ordinary work product [emphasis added]).

Facebook also previously has publicized general statements regarding the ADI reflected in the five requests, thereby further reducing the risk that the disclosure of the names of the apps and some of the additional factual information requested about those apps will reveal confidential opinion work product. See New York Times Co. v. United States Dep't of Justice, 939 F.3d 479, 496 (2d Cir. 2019) ("We first evaluate whether . . . public statements about the memoranda were specific enough to have effectuated disclosure of parts of the memoranda and accompanying exhibits, thereby waiving the work product privilege with respect to those parts"). That being said, the specifics of the five requests and additional information requested must be considered to determine whether fact or opinion work product is being sought, or whether further review is required to make this determination.

We begin with the five requests, and the names of the apps that fall into these requests. They are:

"1. The group of 6,000 apps with a large number of installing users . . . ;

"2. The group of apps and developers that fall within certain categories that, based on Facebook's 'past investigative experience,' present an elevated risk of potential policy violations . . . ;



"3. The group of apps and developers that were reported to Facebook from outside of the ADI process . . . ;

"4. The group of apps and/or developers on which, to date, Facebook has conducted a 'detailed background check' . . . ; [and]

"5. The group of apps on which, to date, Facebook has conducted a 'technical review . . . .'"

Some of this information has been discussed in public statements made by Facebook. Facebook's chief executive officer testified before Congress that Facebook was "investigating every app that had access to a large amount of information" and that it considered "suspicious activity" to be apps that had "a significant number of users and . . . sought to access significant or unexpected data fields." Similarly, in its September 2019 release, Facebook announced to the public that it was conducting "background investigations" and "technical analyses." It also publicized that it was "analyz[ing] potentially suspicious activity from our analysis of logs and usage patterns by these apps" and "conduct[ing] an audit using internal and external experts."

All these public disclosures are important because a corporate defendant cannot publicize its "internal investigation to assert the propriety of its actions to third parties and simultaneously . . . block third parties from testing whether its representations about the internal investigation are accurate." Grand Jury Investigation, 437 Mass. at 354.

Facebook also has provided to the Attorney General more specific information on the ADI framework and an overview of the types of criteria that guide each phase. See In re Steinhardt Partners, L.P., 9 F.3d 230, 235 (2d Cir. 1993) (disclosure of protected thought processes to adversary waives work product protection). This more specific information also helped the Attorney General frame the five requests. In this unusual context, where (1) the underlying facts on the apps and their data breaches are discoverable; (2) the general scope and methodology, and some of the results, of Facebook's internal investigation have been made public as part of its defense of its actions; and (3) Facebook already explained its more specific methodology for conducting its factual investigation to its adversary the Attorney General, it is difficult to discern how opinion work product would be divulged by production of the names of the apps, and most of the other purely factual information requested in the first five categories of apps. See Boehringer II, 778 F.3d at 152, quoting In re San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d at 1015 ("There is no 'real, nonspeculative danger of revealing the lawyer's thoughts' when the thoughts are already well-known"). See also New York Times Co., 939 F.3d at 495, quoting Rockwell Int'l Corp. v. United States Dep't of Justice, 235 F.3d 598, 605 (D.C. Cir. 2001) ("common sense suggests that verbal description of the contents of a document, if sufficiently specific, is as

'inconsistent with the maintenance of secrecy' of that document as would be disclosure of the document itself").

Nonetheless, a careful comparison of the specific factual information requested, and the particular public statements already made regarding the investigatory process, is necessary to determine whether the information requested will reveal counsel's thought processes as well as purely factual information. If undisclosed strategic decision-making by counsel, including the assessment of legal risk or liability, is revealed by the factual analysis, such factual analysis may be classified as opinion work product. A good example of a request posing such risk is the second request, which would force Facebook to identify which apps it determined, based on its "'past investigative experience,' present[ed] an elevated risk of potential policy violations." This reference to past investigatory experience and evaluation of elevated risk of violations appears to seek to reveal undisclosed aspects of the ADI process that may divulge counsel's investigatory practices, legal risk assessment, and other thought processes and impressions. This is quite different from some of the more straightforward factual requests, seeking for example the names and details concerning the 6,000 apps that Facebook has targeted for having a large number of users or the groups of apps that were reported to Facebook outside the ADI process.

Some of the categories of additional factual information requested raise similar concerns. In particular, for some of the apps, the Attorney General is seeking the "basis and initial source(s) of reports, allegations or concerns of data misuse of user information obtained or accessed through the app." Whether at least this last category of additional information seeks to probe into counsel's undisclosed thought processes requires further investigation by the judge.

In sum, we cannot conclude on the record before us that none of the information requested falls into the category of opinion work product, as the judge determined. It is true that the app information here is readily distinguishable from more typical examples of opinion work product, such as the memorandum in Comcast that contained "a detailed analysis of various corporate entities and address[ed] various options, and attendant litigation risks, for [a] stock sale in light of applicable Massachusetts law," Comcast, 453 Mass. at 300, or the memorandum in Schaeffler that analyzed the tax implications of business transactions and included advice related to potential investigation by a Federal agency, Schaeffler v. United States, 806 F.3d 34, 43-45 (2d Cir. 2015). We also recognize that some aspects of the ADI process already have been publicized widely, and Facebook cannot claim protection for opinion work product for investigatory procedures it has publicly proclaimed. See

Grand Jury Investigation, 437 Mass. at 354. See also New York Times Co., 939 F.3d at 496 (public statements describing contents of work product that are "sufficiently specific . . . are tantamount to public disclosure of . . . the relevant [work product]" and therefore constitute waiver). The question that remains is whether some of the factual information about the apps that Facebook is required to produce will reveal any meaningful previously undisclosed attorney thoughts or strategies. See Boehringer II, 778 F.3d at 152, citing In re San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d at 1015. To answer that question, remand is required that compares the specific requests, particularly those identified in this opinion as problematic, the previous public disclosures, and what the particular information requested would reveal. The incomplete record here does not allow us to perform such review ourselves. The judge is also much better positioned than this court to perform this type of document-by-document work product review.<sup>21</sup>

iii. Substantial need and undue hardship. Although further line drawing is required by the judge to determine what

---

<sup>21</sup> Because Facebook has now started to produce information responsive to the first five requests, the judge will be able to review the disclosed information in camera when determining whether the disclosures reveal opinion work product. The judge also may conduct further hearings with counsel to discuss specific requests and the risks of disclosure of counsel's thoughts, impressions, or opinions that they may present.

information requested is fact work product and what is opinion work product, we recognize, based on the record before us, that a significant amount of information ultimately will be determined to be fact work product. We therefore address the issue whether the fact work product must be produced. This requires the Attorney General to demonstrate substantial need and undue hardship. See Mass. R. Civ. P. 26 (b) (3). Absent such substantial need and undue hardship, the Attorney General would be expected and required to do her own investigation. See Baker v. General Motors Corp., 209 F.3d 1051, 1054 (8th Cir. 2000) (fact work product "not discoverable unless the party seeking discovery has a substantial need for the materials and the party cannot obtain the substantial equivalent of the materials by other means" [emphasis added]).

A substantial need exists where the fact information is relevant and the requesting party cannot reasonably obtain the information or its substantial equivalent elsewhere. See Boehringer III, 180 F. Supp. 3d at 14, citing Boehringer II, 778 F.3d at 155. There also must be "'special circumstances' excus[ing] the movant's failure to obtain the requested materials itself." Boehringer II, supra. When interpreting the analogous Federal rule, courts consider, among other factors, "(1) the importance of the materials to the party seeking them for case preparation, (2) the difficulty the party will have

obtaining them by other means, and (3) the likelihood that the party, even if he obtains the information by independent means, will not have the substantial equivalent of the documents he seeks." Burrow v. Forja Taurus S.A., 334 F. Supp. 3d 1222, 1229 (S.D. Fla. 2018), citing Advisory Committee Note (1970) to Fed. R. Civ. P. 26. Ultimately, "[t]he 'substantial need' inquiry requires a careful examination of whether non-disclosure will impair the truth-seeking function of discovery." Boehringer II, supra at 156.

Here, several considerations support the Attorney General's claim of a substantial need for the fact work product. The app information is certainly relevant and important; it is central to the Attorney General's investigation, as it identifies apps that may have misused user data on the prior version of the Platform. See Cahaly, 85 Mass. App. Ct. at 425, citing McCarthy, 463 Mass. at 195 (substantial need exists where work product at issue central to claims). The Attorney General has a mandate to investigate such potential misuse of Massachusetts users' data as well as potential misrepresentations by Facebook, and considerable authority with which to do so. See Exxon Mobil Corp. v. Attorney Gen., 479 Mass. 312, 323-324 (2018), cert. denied, 139 S. Ct. 794 (2019) (Attorney General has "manifest interest in enforcing G. L. c. 93A"). There is also a strong public interest in disclosure in cases in which the Attorney

General is investigating potential unfair or deceptive trade practices involving Massachusetts consumers that is absent in a typical civil dispute. See Boehringer III, 180 F. Supp. 3d at 14, quoting Boehringer II, 778 F.3d at 157 ("in the investigatory context here," Federal Trade Commission "was entitled to learn facts on a broader scale than [that] available to a typical civil litigant").

The great difficulty in obtaining this information also is obvious. Given the scope of the ADI, the millions of apps to be analyzed, and the vast quantity of information at issue, uncovering this otherwise discoverable factual information would be a monumental, if not Herculean, task absent Facebook disclosing the app information. See In re San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d at 1019 ("scope of this massive litigation and its consequent special needs called for unorthodox measures").

Finally, it is unlikely that the Attorney General would be able to obtain the substantial equivalent of this app information, even with extraordinary efforts. As the Attorney General argues, only Facebook has access to the information and data that are necessary to identify the apps that have potentially misused user data. An important part of the ADI framework is Facebook's own knowledge of and experience with the Platform and the apps and developers that operate on it.



Through its design of the Platform and its ongoing efforts to police the Platform, Facebook has developed valuable expertise that has guided the ADI, relying on its own internal knowledge and expertise regarding its Platform and apps to guide its internal searches. Without such expertise, therefore, it is unclear whether the Attorney General would be able to replicate the work of the ADI and identify many of the apps and developers that may be misusing user data.

This is not a case where the internal investigation involved simply interviewing key employees and other witnesses or reviewing a manageable number of documents, tasks that can be easily replicated by third parties or government investigators. See, e.g., In re Int'l Sys. & Controls Corp. Sec. Litig., 693 F.2d 1235, 1240 (5th Cir. 1982) ("discovery of work product will be denied if a party can obtain the information he seeks by deposition"); Gay v. P.K. Lindsay Co., 666 F.2d 710, 713 (1st Cir. 1981), cert. denied, 456 U.S. 975 (1982) ("there is in general no justification for discovery of the statement of a person contained in work product materials when the person is available to be deposed"). Rather, it is an enormously complex effort in which counsel and the ADI team analyzed millions of apps and enormous amounts of data. This analysis was also enabled in large part by Facebook's prior expertise in developing and policing the Platform. Facebook is not only in a

far better position than the Attorney General, but also essentially uniquely positioned to identify which apps potentially misused user data. Therefore, we are persuaded that the Attorney General would be unable to otherwise obtain the substantial equivalent of the factual app information, even with an extraordinary expenditure of time and resources. See Ward v. Peabody, 380 Mass. 805, 817-818 (1980) (that materials are not available from any other source is "favorable to requiring production").

For these same reasons, the Attorney General has demonstrated that she is unable to obtain the requested information or its substantial equivalent without undue hardship. Undue hardship may exist where shielding fact work product would impose extraordinary expense on the requesting party. See, e.g., In re Int'l Sys. & Controls Corp. Sec. Litig., 693 F.2d at 1241 ("[I]n the ordinary case, the cost of one or a few depositions is not enough to justify discovery of work product. . . . But there have been cases in which unusual expense has constituted undue hardship" [emphasis added]). Also relevant is the amount of time it would take to obtain or produce the materials independently. See, e.g., In re Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d at 846 ("considerable delay" factor supporting undue hardship); Resolution Trust Corp. v. Heiserman, 151 F.R.D. 367, 376 (D.

Colo. 1993) (undue hardship exists where it would be "extremely difficult, not to mention wasteful, for defendants to attempt to replicate [opposing party's] three-year investigation" in complex case "involv[ing] massive amounts of documentation").

As explained above, the Attorney General undoubtedly would incur enormous costs and delay in her investigation if the app information is not disclosed. Through the ADI, Facebook has reviewed millions of apps to determine whether they potentially misused user data. When the Attorney General filed the petition to compel in August 2019, the ADI had been operating for nearly one and one-half years. Moreover, so great was the task of the ADI that the investigative team has at times swelled to include hundreds of outside experts. There is no other way for the Attorney General to try to obtain this information other than to essentially recreate and duplicate the work of the ADI. See, e.g., In re Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d at 846 (undue hardship exists where "replication of the [work product] would involve duplication of effort and considerable delay and expense"); Washington Bancorp. v. Said, 145 F.R.D. 274, 279 (D.D.C. 1992) ("the time and money it would take" to review 2,400 boxes of documents to create document index constitutes undue hardship because "no value and only waste in requiring such a duplicative effort"). Facebook acknowledges this reality; its position is simply that the

Attorney General must conduct her own independent investigation for reasons of adversarial fairness. To seek to obtain the app information, therefore, the Attorney General would have to expend an exorbitant amount of public resources and conduct a multiyear investigation to obtain information that Facebook already has in its possession. Such effort and expense is sufficient to demonstrate undue hardship. See, e.g., Collins & Aikman Corp., 256 F.R.D. at 411 ("A page-by-page manual review of ten million pages of records is strikingly expensive in both monetary and human terms and constitutes 'undue hardship' by any definition").

In sum, we conclude the Attorney General has demonstrated both substantial need and undue hardship for the fact work product about the apps.

3. Conclusion. For the reasons described above, we conclude that the first five requests are not covered by the attorney-client privilege, as they do not require the production of communications between Facebook and its counsel. As the sixth request does include communications covered by the attorney-client privilege, Facebook must produce a privilege log as required by the Superior Court judge. We therefore affirm the judge's order in these respects.

We also conclude, however, that the work product doctrine applies to the documents requested, and a remand is required to

determine whether some of the documents requested constitute opinion work product. We therefore reverse and remand the decision of the Superior Court judge concluding that the work product doctrine does not apply and that, even if it did, none of the documents required to be produced would reveal opinion work product. Finally, we conclude that the Attorney General has demonstrated that there is substantial need and undue hardship requiring the production of the documents that do constitute fact work product.

So ordered.